

Secureworks®

The Insider Threat Actor

Briefing Prepared for:
North Carolina Department of IT

October 18th 2018

Secureworks®

Who am I



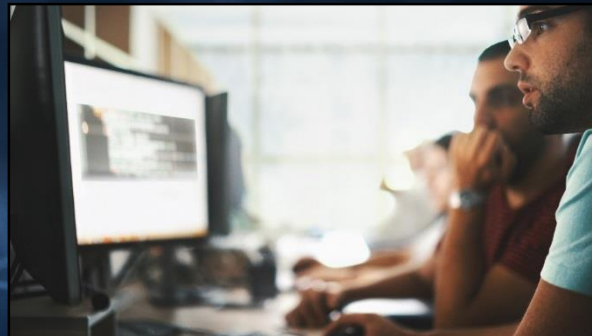
- **United States Military Academy**
- **US Army Signal Corp Officer**
- **VP 13+ Years Financial Services**
- **CIO/CISO 3+ Years Bulk Fuel Distributor**

Secureworks®

3+ Years:

Senior Manager

Threat Intelligence Support



Secureworks®

Secureworks: A brief introduction

Intelligent Security Solutions

Counter Threat Unit™ research team

- Focused on emerging threat trends
- Rapid countermeasure development

Current SOC locations

- Atlanta, Georgia
- Chicago, Illinois
- Providence, Rhode Island
- Edinburgh, Scotland
- Kawasaki, Japan
- 24x7, 365 days/year
- SOC's manned with all teams, working from a single queue
- Disaster recovery
- No client dependency on one SOC

Security Center of Excellence

250B

Events processed
daily

~4,400

Clients

59

Countries

900+

Incident response
engagements
last year

1,800+

Consulting
engagements
performed annually

2,300

Employees

Powered by the Counter Threat Platform™

Agenda

- **What is Insider Threat?**
- **What are the different types of Insider Threat?**
- **What can we do to address Insider Threat?**



Insider Threat

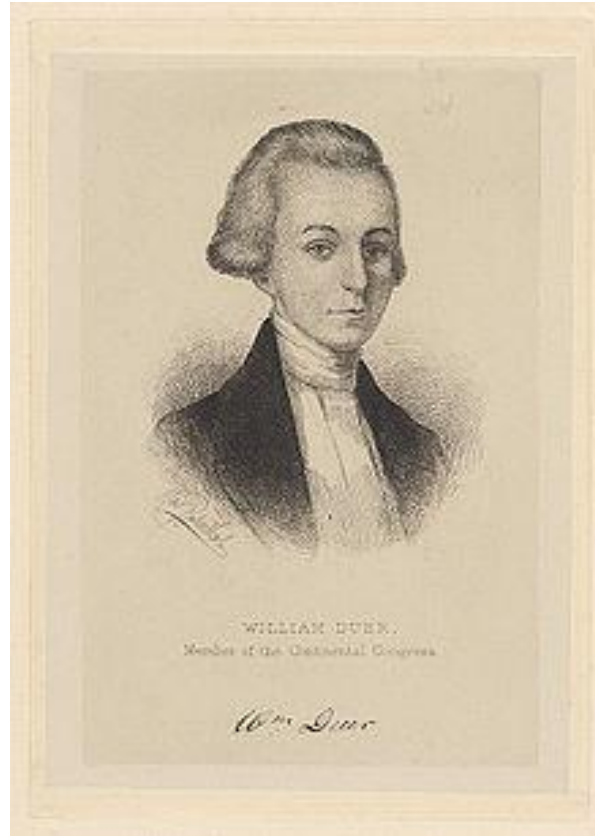
The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

Source: CERT



According to the Ponemon Institute's "2018 Cost of Insider Threats" report, the average cost of insider-caused incidents was \$8.76 million in 2017 — more than twice the \$3.86 million global average cost of all breaches during the same year.

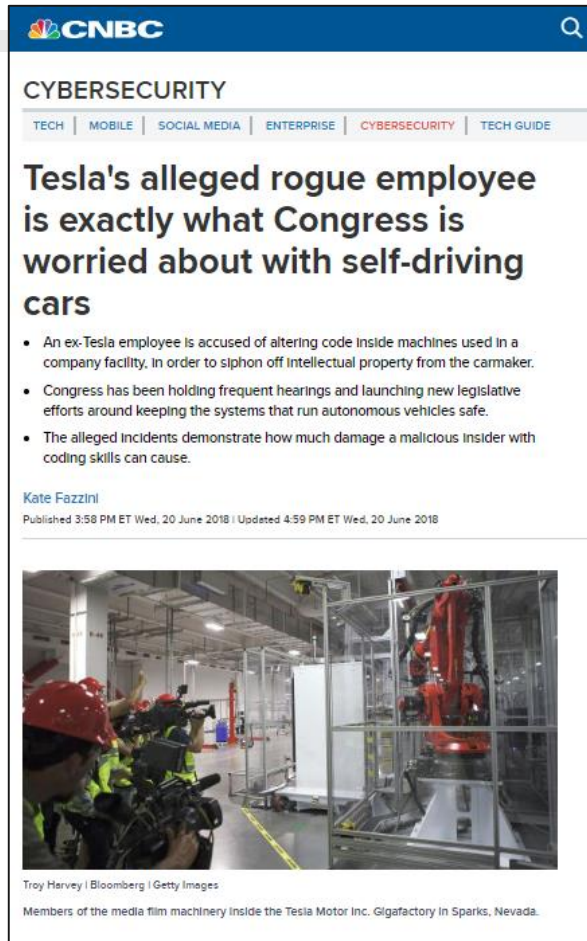
History of Insider Threat



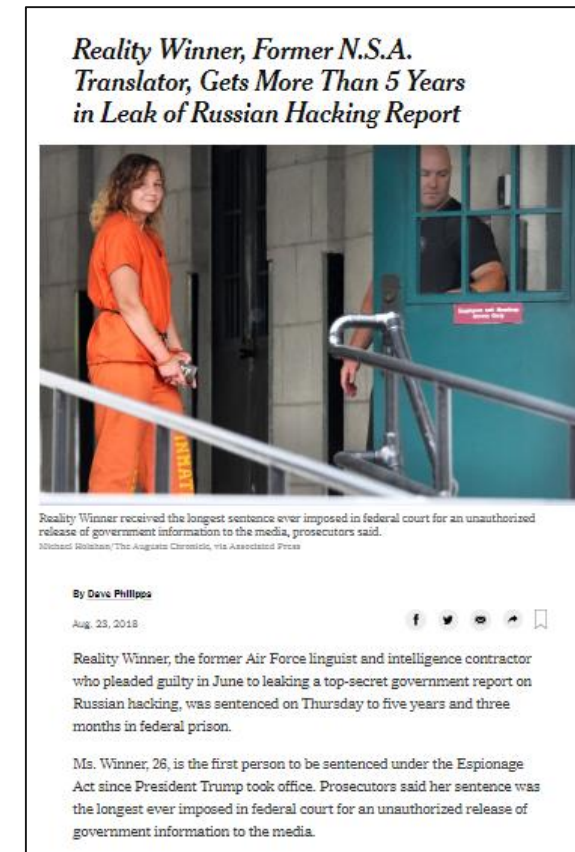
William Duer (1743-1799)
Secretary of the Treasury 1789



Insider Threat continues to be a challenge



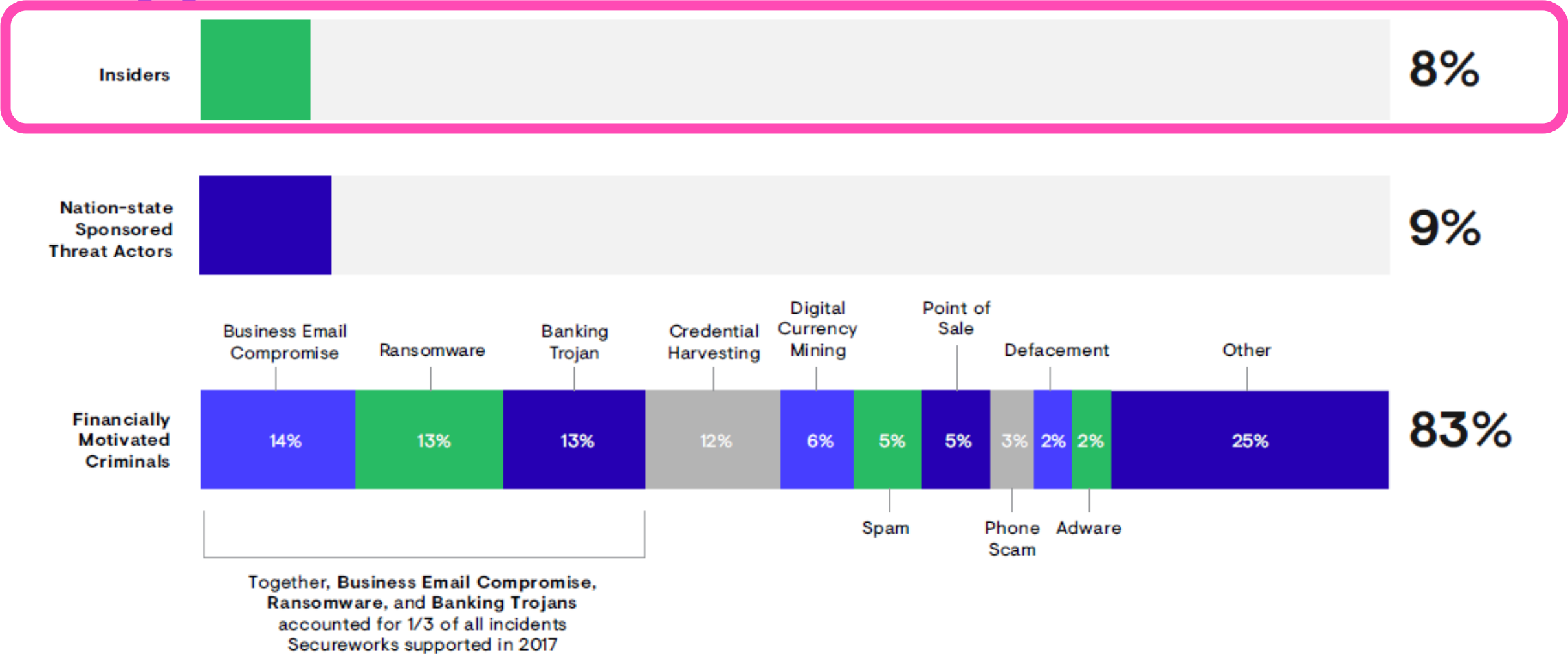
Source: CNBC



Source: New York Times

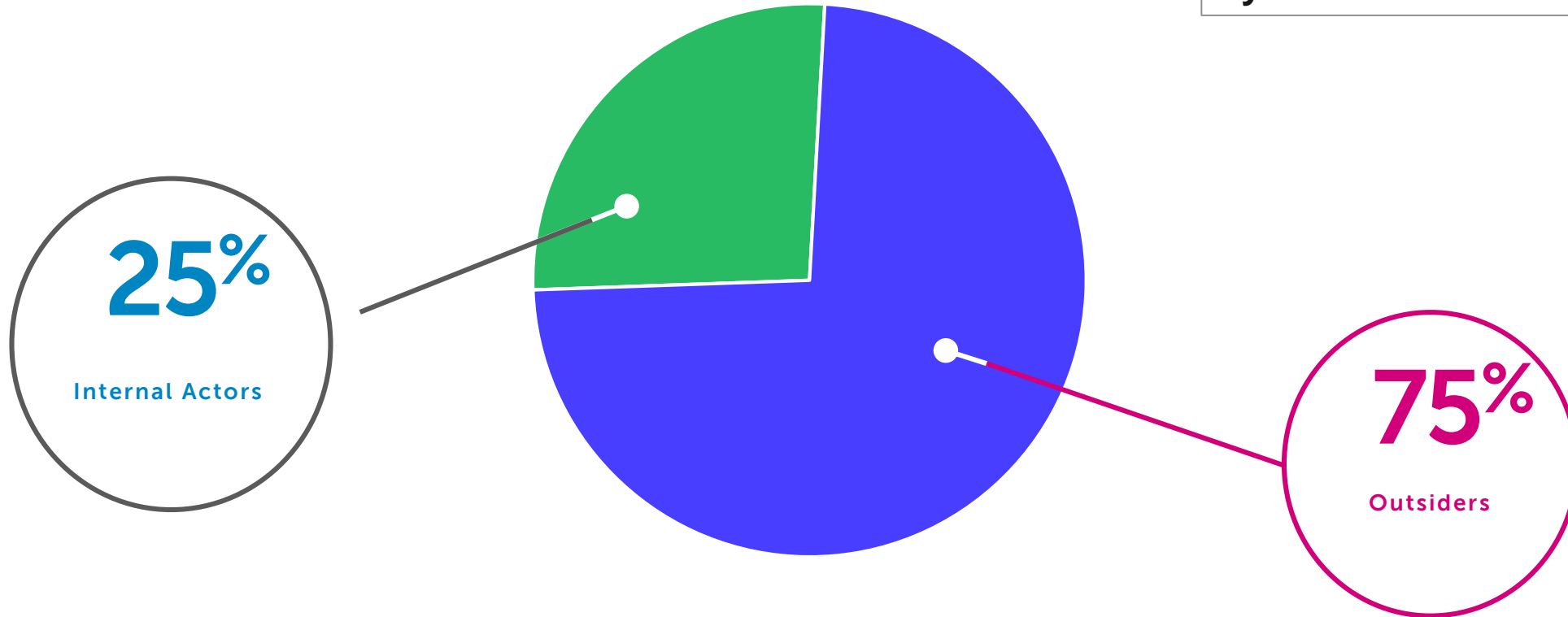
2017 Observed Threats by Secureworks

900+ Engagements, 50TB of evidence collected



Verizon 2018 Data Breach Report

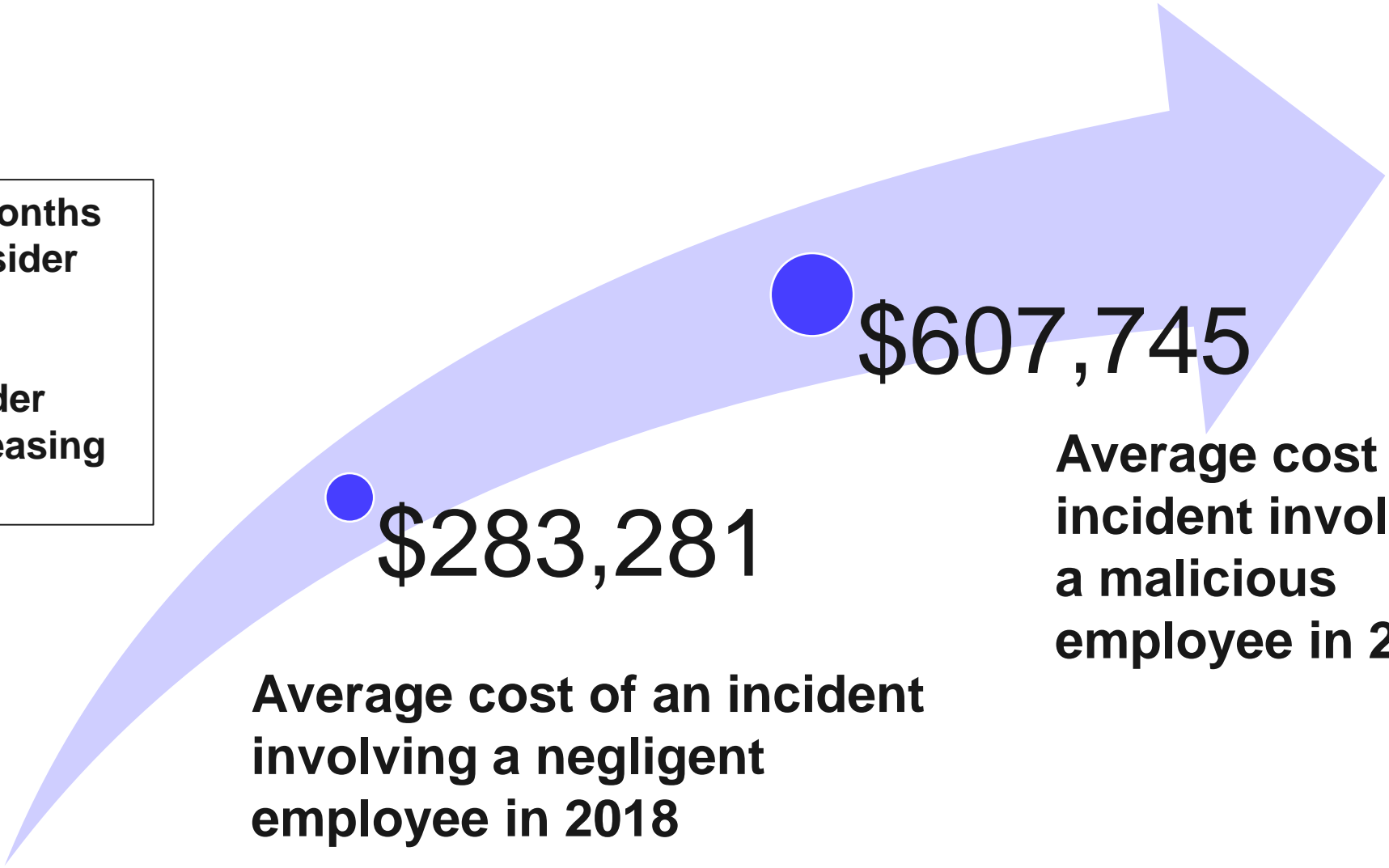
According to CERT 30% of Insider Incidents are detected by non-technical means



Ponemon Institute

**Average of 2+ Months
to contain an insider
incident**

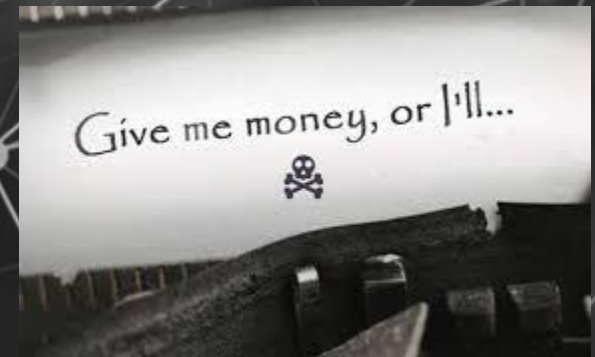
**All types of insider
attacks are increasing
annually**



Can you spot the inside threat?



Potential Motivations for Insider Threat



Categories of Insider Threat

Unintentional Insider

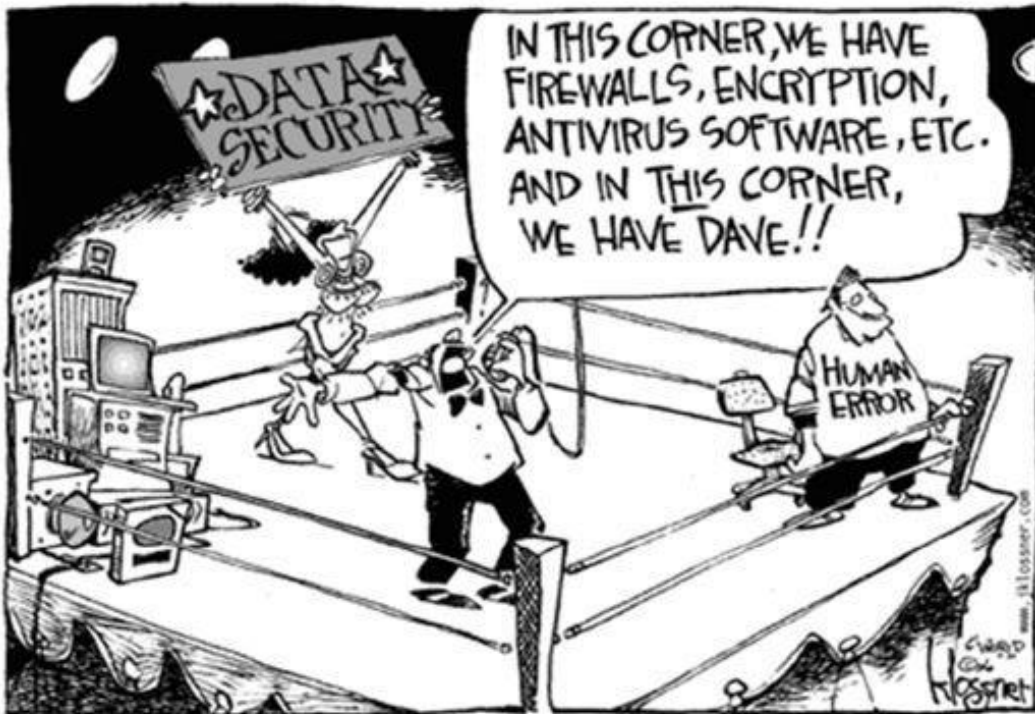
Insider Collusion

Malicious Insider

Disgruntled Employee



Unintentional Insider



Insider Collusion



- Greg Chung
- Employer- Boeing Company (30+years)
- 3000+ pages of technical documents



- Jason Smathers
- Employer – AOL
- 92 Million customer names and email addresses
- In 2003 for \$28k provided list to spammers to promote gambling site



- Reality Winner
- Employer-Pluribus International Corp. – subcontractor for NSA
- Smuggled a TS Government report out in her pantyhose

Malicious Insider



- Anita Collins
- Roman Catholic Archdiocese of NY
- 8 Years – Accounts Payable
- Embezzled over \$1M over seven years



- Linda Lee Clark, 68 Grandmother
- SCICAP Credit Union
- 37 Years- Book Keeper
- Embezzled over \$2.4M

Disgruntled Employee



- Martin Tripp
- Tesla
- Upset he didn't get promotion
- Altered Tesla Code
- Sent "large" amounts of data to unknown parties



- Jo Vito Venzor
- Employer- Lucchese Bootmaker
- Fired from job, took an hour to remove from building
- 1 hour later all IT systems ceased functioning

I'm just a riddle,
wrapped in a mystery,
inside an enigma...

...cloaked in bacon.



som**ee**cards
user card



Possible Insider Threat Behaviors

Remotely Access
Network while on
vacation

Works odd hours-
wants
overtime/weekends

Unnecessarily
copies materials

Interest in matters
outside job duties

Signs of
Vulnerability
(financial, drug,
mental health,
gambling)



Large amounts
of external
email or
network activity

Failed attempts
at accessing
resources

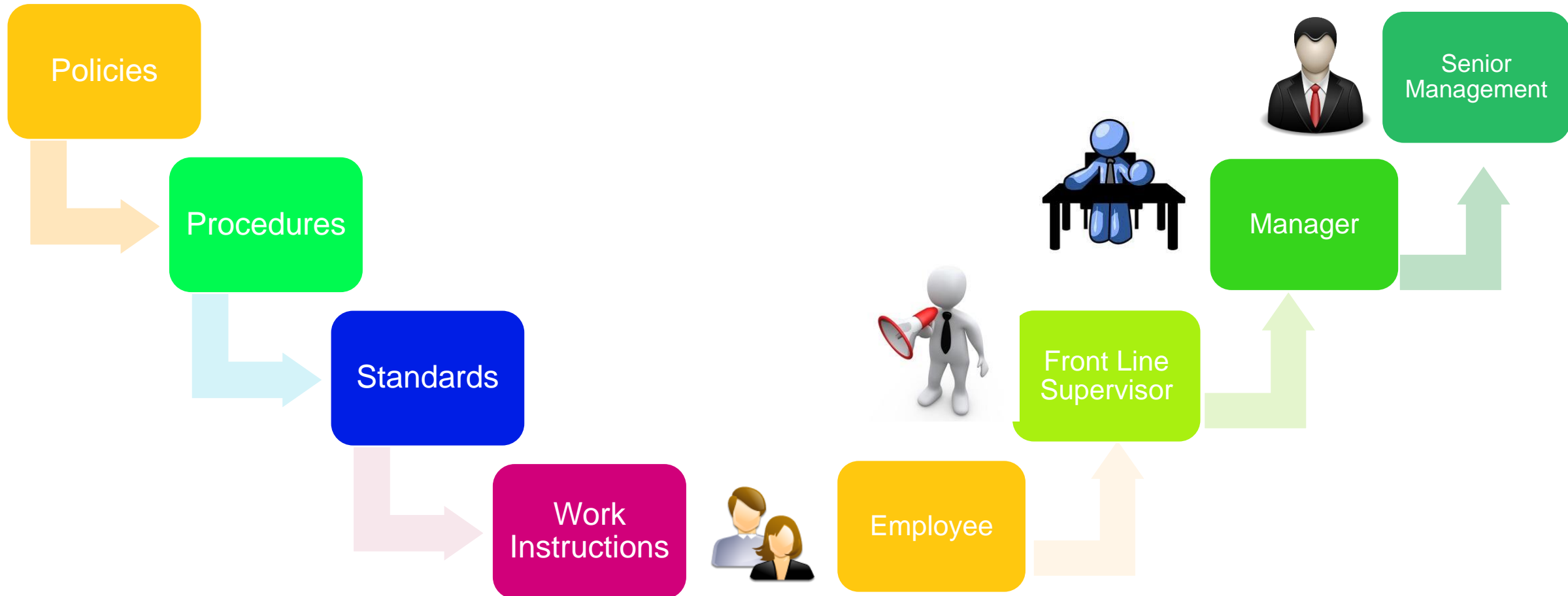
Recent
Disciplinary
Actions

Foreign
contacts/travel

Social Media
Posts

Winning Combination

Top→Down + Bottom→Up Approach



Known Issues

- Policy Violations
- Unauthorized Changes

Suspicious Events

- Unusual work activity
- Unknown error
- Unrecorgnized events

Normal Activity

- Authorized
- Scheduled

Partnership Across the Organization





Not just a technology solution to solve...



Secureworks®

Right Size Access



Trust, But Verify



Periodic Attestation/ Random Spot Checks/ 2 Party Review



See something, Say Something

Positive Incentives more impactful then consequence driven management



Secureworks®

Don't forget the simple things....



facebook



twitter



LinkedIn®

Final Thoughts



There is no single approach that can mitigate all categories of human risk.



Managers- Get to know your people



Establish a culture of self reporting is acceptable.



Start with Data Protection- Identify and classify assets. Build monitoring and safeguards.



Keep HR/Security/IT in the loop with employee actions (Probation/Termination, etc)

Questions

The background of the slide is a dark blue gradient. Overlaid on this is a complex network of thin, light blue lines that connect numerous small, glowing yellow circular nodes. These nodes and lines are distributed across the entire frame, with a higher density of connections on the right side, creating a sense of a global or digital network.

Jeremy Manning
Advisory Security Engineer
Secureworks | Counter Threat Unit(CTU)
jmanning@secureworks.com /www.secureworks.com
O:+1 770.870.3160 /C:+1 832.817.8239

Secureworks®